Penetration Testing Report: Trojan Horse Analysis of Suspicious Link Sent by Nick [redacted]

Report:1

Introduction

This report provides the key findings from a security investigation into a suspicious link sent by Nick [redacted] to the client. The investigation reveals that the link, initially appearing to lead to a Spotify track, was used as part of a Trojan horse attack. The attack aimed to compromise the client's device by disguising malicious activity behind a seemingly legitimate link.

Note:
The detailed analysis supporting these findings is provided in **Report 1**, covering pages **69 to 80**. This section offers an in-depth examination of the technical evidence, including traffic analysis, network communication, and the identified Trojan horse attack vectors. The information summarized in this overview serves as a foundational understanding for **Report 2**, where additional evidence and further investigation are presented.
For a comprehensive analysis of the Trojan horse attack mechanisms and supporting technical data, please refer to **Report 1** (pages 69-80), which is attached to this document.

Link Overview

- **URL:** `https://open.spotify.com/track/4VXIryQMWpIdGgYR4Tr`
- **Source**: Sent by Nick [redacted] to the client.

Initial Observation

At first glance, the URL appears to direct users to a Spotify music track. However, a detailed analysis flagged unusual activity, including traffic to external servers unrelated to Spotify, which is indicative of a Trojan horse attack.

Key Evidence of Attack

1. Suspicious Network Traffic

Upon clicking the link, network traffic to multiple third-party servers was observed. These servers are not connected to Spotify's infrastructure, raising significant concerns:

- **IP: 34.237.241.83:443 (Amazon Web Services)**
  Attackers often use cloud services like AWS to mask malicious activities. The IP traffic suggests the link was designed to communicate with an external server to deliver a Trojan payload.
- **IP: 204.79.197.203:443 (Microsoft)**
  While Microsoft is a legitimate service provider, attackers sometimes exploit trusted platforms for malicious communication. The traffic to this IP after clicking the link supports the theory that the link is part of a Trojan scheme.

- **IP: 23.40.140.168:443 (Akamai Technologies)**
  Akamai is used for content delivery, but in this case, it could serve as a means to distribute malicious payloads.
- **UDP Traffic to Google DNS (8.8.8.8:53)**
  DNS requests to public servers may indicate an attempt to disguise malicious communication with a command-and-control server, commonly associated with Trojan horse malware.

Proof of Intent